"Design and Development of Algorithms for Secure Data Transmission using IoT Devices"

For Degree of Philosophy in Computer Science Under faculty of Science & Technology

Synopsis

Submitting to

Swami Ramanand Teerth Marathwada University, Nanded

Submitted By

Faheemuddin Ahmed

Research Scholar

Under Guidance of

Dr. Nayana. S. Ratnaparkhi

Assistant Professor

Dnyanopasak Shikshan Mandal's Arts, Commerce and Science College, Jintur - 431509

ABSTRACT :

Providing security for the IOT environment is the major assessment carried out where the entire world is dependent on e-communication and assures the guarantee of communication without any error causing .In this work, Raspberry Pi, an open source and a popular choice asthe hardware platform for IoT - both devices as well as gateways, has been used. This research work is carried out for proposing secure communication with IoT devices. The proposed system architecture manages interaction of the receiver with the cloud. This interaction ensures proper authentication through the mechanisms and api(s) provided by the cloud service providers, and these mechanisms are also integrated into the simulation. The cloud services used in the system architecture, that is, cloud messaging as a service, and cloud database as a service ensure that the sender's identity is verified. In this way a blanket authentication system is set up for the mentioned IoT architectures. It enables secure communication between the IoT device and cloud messaging service provider and the mobile device used to send data from IoT Node sensor to the mobile device. Secure authentication while communicating data between sender and receiver nodes is a key concept when providing Internet of Things as a service. Hash algorithms can provide such an authentication mechanism for IoT based applications. This hash code serves as the authenticating token for the transaction. Mechanisms for the sender receiver interaction are built into the program codes in both the simulated communication models. Showcasing the time-series formatted data using Visualization tool Grafana and NOSQL cloud database AWS DynamoDB.

INTRODUCTION:

The number of active IoT devices is expected to be 10 billion in the year 2020 and is further expected to rise to a massive 22 billion by the year 2025 [1]. This illustrates the potential of the Internet of Things. One such IoT device, raspberry pi [2], is a low cost and versatile computer that has the potential to make Internet of Things more accessible to the developing countries. It is a device capable of acting as both the end node in an IoT network, and as an analytical machine and a central server for a small IoT network. It offers python programming language support. There are two popular IoT communication models namely publish subscribe and request response[3].

A publish subscribe model with an MQTT [4] broker. MQTT (Message Queue Telemetry Transport) is an application protocol viewed as a publish subscribe model, designed for thecommunication of M2M .This protocol sits on top of TCP/IP layer. Both client and broker need to have a TCP/IP protocol stack. MQTT broker acts as a server in this model and both publisher and subscriber are the clients. A broker maintains the list of topics to which various publishers publish information. A subscriber subscribes to a topic of interest and can asynchronously obtain the messages from the broker. A publisher will be a sensor hardware that sends sensed data[5]. A subscriber will be a machine that does further processing with the received data. A publish subscribe architecture is useful for remote communication wherethe network band width is constrained and a light code footprint is desired. It is a client servermodel, where MQTT broker as server and publisher and subscriber as a client. This model is also useful when there are many nodes sending and receiving data in a heavy traffic environment.

On the other hand Request response communication model, is a tried and tested model that works well in a low traffic setting. Publish subscribe model is asynchronous whereas the request response model is synchronous. Although the publish subscribe model is flexible and the message can stay in the message queue[6] of the broker for some time while the receiver is busy, it is prone to memory buffer overflow for a constrained memory broker. On the plus side, for a publish subscribe model deployed in highly critical applications, critical data will be available in the broker even if the receiver is busy. However for a request

response model in a critical application, there is a possibility of unproductive pinging between the receiver and the sender to continuously stay up to date [7].

SHA-3 (SHA-3 is a subset of the broader cryptographic primitive family Keccak) provides a secure mechanism for creating a unique signature for data transaction, a hash code that is unique to this transaction. SHA-3 is the most recent among the hash algorithms standardized by National Institute of Standards and Technology (NIST). SHA-3 is currently the most secure hash algorithm. SHA -3 provides authentication of the data over the internet. A hash function is a mathematical operation that takes a plain message data of a variable length and provides a fixed size of hash message value. Hash algorithm is useful for data integrity and security. An integration of the IoT system with the cloud is indispensable to the current times. If some critical information needs to be communicated by the receiver machine to some remote client, say an android device, a cloud messaging service can assist in sending an appropriate notification. Simultaneously, the system can upload necessary data to a cloud database[8].

AIM AND OBJECTIVES OF STUDY:

- Implementation of Hash Authentication mechanism.
- Design and development of new algorithms for secure data transmission.
- Testing new algorithms and comparison with other methods.
- Capture data from IoT sensors and transmit in a secure way and forward to the cloudmessaging service.
- Study signature based SHA-3 hash algorithm.
- Implementation of notification service delivery via Push notifications.
- Implement publisher subscriber consumer pattern in IoT node (software side) viaMQTT.
- Showcase the visualization of Sensor data using Grafana and secure storage of AWSDynamoDB.

REVIEW OF LITERATURE:

1. Aarti Goel, Deepak Kumar Sharma, Koyel Datta Gupta, “LEOBAT: Lightweight encryption and OTP based authentication technique for securing IoT networks” , this research work states that , Authentication is one of the foremost pillars in the Internet of Things (IoT) security that authenticates the identity of a device or a person with the help of a unique identification number. If authentication is compromised then an intruder can gain access and launch a variety of attacks on the network. The world of IoT devices is benefiting us in many ways, but the vulnerability of becoming a victim of cybercrime is also increasing at a rapid pace. This research paper proposes an authentication-based solution for designing a secure communication network to ensure safe access to data and stop attackers from any unauthorized access to various IoT applications using cryptography and cloud computing. The proposed work is then compared with other popular cryptosystems such as Secure Internet of Things (SIT), Data Encryption Standard (DES) and Blowfish. LEOBAT is simulated using MATLAB and proves to be a fast and efficient authentication technique.

2. In the research ,”EVOLUTION AND ANALYSIS OF SECURE HASH ALGORITHM (SHA) FAMILY”, the authors explains that, With the rapid advancement of technologies and proliferation of intelligent devices, connecting to the internet challenges have grown manifold, such as ensuring communication security and keeping user credentials secret. Data integrity and user privacy have become crucial concerns in any ecosystem of advanced and interconnected communications. Cryptographic hash functions have been extensively employed to ensure data integrity in insecure environments. Hash functions are also combined with digital signatures to offer identity verification mechanisms and non-repudiation services. The federal organization National Institute of Standards and Technology (NIST) established the SHA to provide security and optimal performance over some time. The most well-known hashing standards are SHA-1, SHA-2, and SHA-3. This paper discusses the background of hashing, followed by elaborating on the evolution of the SHA family. The

main goal is to present a comparative analysis of these hashing standards and focus on their security strength, performance and limitations against common attacks. The complete assessment was carried out using statistical analysis, performance analysis and extensive fault analysis over a defined test environment. The study outcome showcases the issues of SHA-1 besides exploringthe security benefits of all the dominant variants of SHA-2 and SHA-3. The study also concludes that SHA-3 is the best option to mitigate novice intruders while allowing better performance cost-effectively.

3. This authors in their studies Secure transmission technique for data in IoT edge computing infrastructure Rohit Sharma and Rajeev Arya

   The utilization of IoT technology has been rapidly increased in various applications such as smart city, smart banking, smart transport, etc. The internet of things allows the user to collect the data easily using the different sensors installed at various locations in the open environment. The data collection process by the IoT sensors is giving access to the various services. However, due to the open communication medium, it is difficult to provide secure access to these services. In this paper, a data transmission technique has been proposed, which will provide secure communication in IoT infrastructure for smart city applications. In this method, each IoT sensor has toprove their legitimacy to the reader and the base station before the transmission of data. Hence, the IoT sensors can transmit the required data in a secure and efficient way. In the proposed technique, the proof of correction shows that the required information is not supposed to be sent through an online medium, it is obtained at the receiver using the Euclidean parameters shared by the IoT sensors. The proposed technique is compatible to provide security against most of the attacks performed by the attackers. Two random variables and complex mathematical calculation are making the proposed technique more reliable than others. This technique will significantly improve the security of different data transmission services which will be helpful to improve the smart city infrastructure.

4. This authors in their studies Similarity Learning-Based Supervised Discrete

Hash Signature Scheme for Authentication of Smart Home Scenario N Jeyanthi1 and K Swapna Sudha2

Smart home technology is one of the significant emerging applications in the Internet of Things that facilitates the user to control home devices in the remote manner. In this context, investigating and addressing IoT security issues is highly challenging as the operating strategies of IoT applications differ due to their heterogeneity characteristics. At this juncture, an authentication mechanism with anonymity and efficiency is necessary for facilitating secure communication in the smart home scenario, since the user or home communication channels are generally determined to be highly insecure. In this paper, Similarity Learning-Based Supervised Discrete Hash Signature Scheme (SLSDHS) is proposed for achieving secure users during the process of smart home authentication. It leverages the mutual association between possible semantic labels in order to learn maximized more stable hash codes, which is a predominant improvement over the traditional hashcode approaches. The communication overhead and computation overhead of the proposed SLSDHS is identified to be considerably minimized compared to the benchmarked schemes used for comparison. The security analysis of the proposed SLSDHS scheme evaluated using informal analysis, formal analysis, and AVIPSA tool-based model checks confirmed its predominance with respect to automated testing of internet security protocols.

5. In this research paper the authors have demonstrated the use of raspberry pi as a video server, showing the machine's computational abilities. The publish subscribe model isdiscussed in [9]. The authors present an adaptive river monitoring system using the publish subscribe model. Here, even though monitoring of huge amounts of video data is done, the IoT communication is still resource efficient. Hashing and its properties are discussed in detail in [10]. Computational complexity universal hashinghas been discussed in [11]. The problem of sensitive data exposure in IoT has been addressed by the authors of [12]. A hardware serialization-based authentication scheme for IoT based applications is discussed by the authors of [13].

METHODOLOGY TO BE ADOPTED:

1. Configuration of sensor and IoT device, thus enabling to capture the sensor datausing the GPIO programming for Raspberry pi.
2. Analyzing data received from the sensor for accuracy.
3. Encrypting the information using SHA-3 Hash Algorithm.
4. Enabling MQTT messaging queue service for implementation at the raspberry pisystem level.
5. Transmitting data to cloud messaging service and then posting the message to thelistening subscriber on the mobile app side.
6. Showcasing the sensor data received in time-series format using AWS Dynamodbwith Visualization layer provided by Grafana

SCOPE AND SIGNIFICANCE OF THE STUDY:

Smart Homes

IoT encrypted device can provide you insights into your everyday water usage, your set-top box that allows you to record shows from remote, Automatic Illumination Systems, Advanced Locking Systems, and Connected Surveillance Systems

Smart City

Vital concerns like Traffic Management, Waste Management, Water Distribution, Electricity Management, and more. All these work towards eliminating some day-to-day challenges faced by people and bring in added convenience, all data being encrypted and secured via HASH Algorithms

Self-driven Cars

The cars use several sensors and embedded systems connected to the Cloud and the internet to keep generating data and sending them to the Cloud for informed decision-making through Machine Learning, The communication between different sensors can be encrypted in a manner that is it impossible for any malware or any

other hacking device to interpret the messaging passed between the sensors and CPU, Thus enabling secure environment for the communication between sensors.

Wearables

Wearables remain a hot topic in the market, even today. These devices serve a wide range of purposes ranging from medical, and wellness to fitness. Of all the IoT startups, Jawbone, a wearables maker, is second to none in terms of funding. These devices too comes with different sensor based communication, eg) oximeter, pulsemeter, heart rate monitoring making it crucial example to implement data security for the data captured from sensors to the pr.

PROBLEM STATEMENT:

This work discusses a blanket authentication scheme for publish subscribe and request response based IoT architectures that extend to cloud based services. The authentication of data in the interaction between the sender and the receiver in both these communication models is ensured by SHA -3 algorithms. This mechanism creates a unique signature for each data transaction between the sender and the receiver.

The interaction between the receiver and the cloud is secured via the mechanisms provided by the cloud service providers. A push notification is successfully delivered to the remote client device via a cloud messaging service by using a unique token for authentication generated during the initial handshake between the device and the service. Updates done to the cloud database by the receiver for the verified authentic data received from the sender are also authenticated by the usage of a private key generated during the initial cloud database setup. This blanket authentication system is efficient and state of the art, and can be deployed into the real world. This would be really useful providing a working prototype of Secure communication between IoT devices and the network to the receiver device. The proposed work also showcases how the sensor data can be visualized in a secure way using secure communication between AWS DynamoDB and Visualization tool Grafana in order to show the sensor data in a time-series format.

PROPOSED WORK PLAN/ FORMULATION AND STRUCTURE OF STUDY:

Year-wise Plan of work and targets to be achieved:

2021-2022:

- Literature Review of related topics.
- Study of different methods of securing communication between IoT devices.
- Participate in Seminar/Conferences/Training Related Subjects.
- Online coursework.

2022-2023:

- Study & Setup of cloud messaging and storage services.
- Study of Python Programming Language to implement GPIO Programming forRaspberry Pi.
- Study of Temperature & Humidity sensor and communication programming.

2023-2024:

- Data Collection for the study.
- Two or Three Research Papers published.
- Grafana Visualization and AWS DynamoDB Storage

2024-2025

- Implementation of Secure Communication Hash Algorithms using IoT devices andsensors.
- Implementing prototype for showcase of secure communication of IoT devices.

REFERENCES:

1.	psycopg2 - python-postgresql database adapter [internet]. Available from:https://pypi.org/project/psycopg2
2.	Aarti Goel, Deepak Kumar Sharma, Koyel Datta Gupta, "LEOBAT: Lightweight encryption and OTP based authentication technique for securing IoT networks",https://onlinelibrary.wiley.com/doi/10.1111/exsy.12788, 29 july 2021
3.	Research Paper Secure hash authentication in IoT based applications : International Journal of Advanced Research in Computer and Communication Engineering ISO3297:2007 Certified Vol. 5, Issue 7, July 2016
4.	Firebase-admin 2.17.0 [internet]. Available from: https://pypi.org/project/firebase-admin/
5.	Set up a firebase cloud messaging client app on android .Available from: https://firebase.google.com/docs/cloud-messaging/ android/client.
6.	Similarity Learning-Based Supervised Discrete Hash Signature Scheme for Authentication of Smart Home Scenario: https://iopscience.iop.org/article/10.1149/10701.13311ecst
7.	Li, Wu-Jeng, Chiaming Yen, You-Sheng Lin, Shu-Chu Tung, and ShihMiao Huang. (2018) "Justiot internet of things based on the firebase real-time database." International Conference on Smart Manufacturing, Industrial & Logistics Engineering(SMILE): IEEE: 43–47
8.	Secure transmission technique for data in IoT edge computing infrastructure:https://link.springer.com/article/10.1007/s40747-021-00576-7
9.	psycopg2 - python-postgresql database adapter [internet]. Available from:https://pypi.org/project/psycopg2/
10.	pysha3 1.0.2, sha-3 wrapper (keccak) for python [internet]. Available from:https://pypi.org/project/pysha3/

11.	Frikken, Keith B., Marina Blanton, and Mikhail J. Atallah. (2009) "Robust authentication using physically unclonable functions." International Conference onInformation Security: Springer: 262–277.
12.	Set up a firebase cloud messaging client app on android .Available from: https://firebase.google.com/docs/cloud-messaging/ android/client.
13.	psycopg2 - python-postgresql database adapter [internet]. Available from:https://pypi.org/project/psycopg2/.
14.	Burhan Ul Islam Khan, Rashidah Funke Olanrewaju, Malik Arman Morshidi, Roohie Naaz Mir, Miss Laiha Binti Mat Kiah, Abdul Mobeen Khan, "EVOLUTION AND ANALYSIS OF SECURE HASH ALGORITHM (SHA) FAMILY", Published: Jul 27, 2022.
15.	Lueth, Knud L.(2018) State of the iot 2018